REMARKS

Claim Objections

The Examiner objected to the use of a British English spelling of the word "organisation". The Applicant respectfully notes that the use of British English spellings is quite acceptable. See MPEP § 608.01. Kindly withdraw the objection.

Claim Rejections under 35 USC § 112

Claims 23-28 were rejected under 35 USC § 112, second paragraph, because the limitations of the independent claims were not recited positively. Claims 23 and 28 have been amended to recite the claim limitations more positively. Additionally, a step of "forming said data set using at least the encrypted first and second items" has been added to each of these claims to more closely follow the form of related apparatus claims 43 and 47.

Claim Rejections under 35 USC § 103

The examiner relies on two references, namely US Patent Publication 2004/0098589 (Appenzeller) and US Patent Publication 2003/0081785 (Boneh); the latter reference is the patent version of the seminal paper by Boneh & Franklin mentioned at line 29, page 4 of the present application. Neither reference discloses or suggests the present invention though both are concerned with IBE (Identifier-Based Encryption).

In identifier-based encryption, the data to be encrypted is encrypted using as encryption parameters:

- **public data** of a trusted party;
- **an encryption key string** – this can be any arbitrary string and does not need to be known in advance by the trusted party (the trusted party is responsible for generating the corresponding private key).

The private key is generated by the trusted party using:

- **the encryption key string;**
- **private data** of the trusted party, this private data being related to the public data of the trusted party.

Using the public data of the trusted party as an encryption parameter ensures that only that trusted party can generate the private key needed for decryption.

Appenzeller relates to a fairly standard IBE system but discloses the use of multiple private key generators PKGs (similar to the trusted authorities of the present application). The contribution of Appenzeller appears to be the provision of directory services for providing a sender associated with one PKG with appropriate public parameters to use when encrypting messages for a receiver that is associated with a different PKG.

With regard to the passages of claim 23 that, after amendment, read:

> "encrypting a first item, according to an Identifier-Based Encryption, IBE, scheme, in dependence on encryption parameters comprising a first encryption key string that identifies said specific individual, and public data of a first trusted authority competent in respect of professional accreditations;
>
> encrypting a second item, according to an IBE scheme, in dependence on encryption parameters comprising a second encryption key string that identifies said specific organisation, and public data of a second trusted authority competent in respect of accreditations of organisations;"

the Examiner cites (or likely would cite) four paragraphs of Appenzeller as being relevant, namely [0047], [0070], [0076], & [0079]. These paragraphs say little more than that there are multiple PKGs each generating private keys for respective users based on the identities of users, and that a directory service

enables a message sender to discover the public parameters of the PKG associated with an intended message recipient. Apart from the fact, acknowledged by the Examiner of page 4 of the Official Action, that Appenzeller does not explicitly disclose a first PKG "competent in respect of professional accreditations" and a second PKG "competent in respect of accreditations of organisations", Appenzeller does disclose the basic features of the quoted claim passages.

Concerning the competences of the PKG, the Examiner tries to use Boneh's paragraphs [0053], [0054] to fill the gap. These paragraphs just do not fill the gap. These paragraphs do not suggest a first PKG "competent in respect of professional accreditations" and a second PKG "competent in respect of accreditations of organisations".

With regard to the passages of claim 23 that, after amendment, read:

> "forming said data set using at least the encrypted first and second items;
> recovery of the target data in clear requiring decryption of both the first and second items."

the examiner cites two paragraphs of Appenzeller as relevant, namely [0058] & [0068]. However, paragraph [0058] of Appenzeller simply describes how to encrypt data according to an IBE scheme using bilinear maps (in fact, this seems to be a rather general description of the well known "BasicIdent" method described at paragraph [0115] *et seq.* of Boneh. Paragraph [0068] of Appenzeller is concerned with incorporating a time element into a user's identity in order to force them to request a new decryption key at regular intervals.

Neither paragraph [0058] nor [0068] of Appenzeller has anything to say about:

forming a data set comprising two items IBE encrypted using the public parameters of different PKGs; or

the inter-relationship between these two items and the encrypted target data, namely that both items must be decrypted in the course of recovering the target data in clear.

Appenzeller therefore fails to disclose or suggest the invention set out in claim 23. Furthermore, the Examiner has not pointed in anything in Boneh which fills in any of the gaps in Appenzeller.

The same arguments apply to claims 28 and 43.

With regard to independent claims 48 and 54, these claims are related to claims 23, 28 and 43, but at the same time they rather differ from those claims. Claims 48 and 54 are concerned with what a requesting party does to decrypt the target data from the data set whereas claims 23, 28 and 43 are concerned with encrypting the first and second items when creating the data set. So they are related, but at the same time different.

The Examiner has cited against independent claims 48 and 54 the same paragraphs of Appenzeller that he used against claims 23, 28, 43.

The easiest thing to say with respect to claims 48 and 54 is that Appenzeller (and in particular paragraphs [0058], [0068] thereof) does not disclose or suggest the following limitation found in each of these two independent claims:

> "third means for using the first decryption key, or the first item, provided by the first trusted authority and the second decryption key, or the second item, provided by the organisation, to recover the target data"

It is not too surprising that this limitation (regarding recovering the target data) is not met, given the fact that the Examiner failed to show where Appenzeller teaches forming the data set in the first place.

In view of the foregoing, further discussion of the rejections of independent claims 48 & 54 (or their dependent claims) is not apropos at this juncture.

Reconsideration of this application as amended is respectfully requested.

I hereby certify that this correspondence is being deposited electronically with the United States Patent and Trademark Office on

21 October 2008
(Date of Transmission)

/Lonnie Louie/
(Name of Person Transmitting)

(Signature)

21 October 2008
(Date)

Respectfully submitted,

/Richard P. Berg 28145/

Richard P. Berg
Attorney for the Applicant
Reg. No. 28,145
LADAS & PARRY
5670 Wilshire Boulevard,
Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile